UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/844,246	04/30/2001	Yves Louis Gabriel Audebert	741.01101	8917

7590 11/01/2007

STEVENS, DAVIS, MILLER & MOSHER, LLP
1615 L Street, N.W., Suite 850
Washington, DC 20036

EXAMINER
LANIER, BENJAMIN E

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
11/01/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	09/844,246	AUDEBERT ET AL.
	Examiner	Art Unit	
	Benjamin E Lanier	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>22 October 2007</u>.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-7,9,10 and 15-42</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-7,9,10 and 15-42</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>31 July 2001</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Response to Arguments

1.   Applicant's argument that DiGiorgio in view of Coulier teaches encapsulated packets

between the local computer and smart card, as opposed to encapsulated packets between the

local computer and remote computer, has been fully considered and are persuasive. Therefore,

the rejection has been withdrawn. However, upon further consideration, a new ground(s) of

rejection is made in view of DiGiorgio, U.S. Patent No. 6,385,729, in view of Elgamal, U.S.

Patent No. 5,657,390.

Claim Rejections - 35 USC § 103

2.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

3.   The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459

(1966), that are applied for establishing a background for determining obviousness under 35

U.S.C. 103(a) are summarized as follows:

1.   Determining the scope and contents of the prior art.
2.   Ascertaining the differences between the prior art and the claims at issue.
3.   Resolving the level of ordinary skill in the pertinent art.
4.   Considering objective evidence present in the application indicating obviousness
        or nonobviousness.

4.   Claims 1-7, 9, 10, 15-17, 19-39, 41, 42 are rejected under 35 U.S.C. 103(a) as being

unpatentable over DiGiorgio, U.S. Patent No. 6,385,729, in view of Elgamal, U.S. Patent No.

5,657,390. Referring to claims 1, 42, DiGiorgio discloses a secure token device access system

wherein a secure token device and a local computer system communicate via a token reader, and

by passing data packages known as application protocol data units (APDUs) using the reader

(Col. 1, line 63 – Col. 2, line 13 & Col. 9, lines 1-6), which meets the limitation of client

communications means for transmitting and receiving message packets over said network using a

packet based communications protocol, and for transmitting and receiving APDUs through said

PSD interface. When a user attempts to access ISP services from the token device, the ISP issues

a challenge to the token device to ensure that the user should be granted access to the ISP

services (Col. 2, lines 16-23 & Col. 10, lines 24-33), which meets the limitation of a first client

data processing means for receiving incoming message packets from said remote computer

system using said client communications means, separating APDUs from said incoming message

packets thus generating APDUs and routing said APDUs to said PSD through said PSD Interface

independently of the origin and integrity of said incoming message packets. Once the challenge

is received at the token device, the token device issues a response to the ISP challenge in the

form shown in Figure 8B (Col. 10, lines 33-35), which meets the limitation of second client data

processing means for receiving incoming APDUs from said PSD interface, incoming APDUs

into outgoing message packets and routing said outgoing message packets to said remote

computer system through said client communications means. DiGiorgio discloses that the local

computer communicates with the remote computer using a web browser (Abstract) over the

network. DiGiorgio does not disclose that the packets transmitted between the local computer

and remote computer are encapsulated. However, it would have been obvious to one of ordinary

skill in the art at the time the invention was made to encapsulate the packets transmitted from the

local computer to the remote computer in DiGiorgio using SSL in order to provide a security in

communications over networks that is platform independent, that can work with many different

types of applications that request a wide variety of different types of server applications, and

which can be performed with minimal time and effort as taught by Elgamal (Col. 1, lines 11-19,

39-55).

Referring to claim 2, DiGiorgio discloses a secure token device access system wherein a

secure token device and a local computer system communicate via a token reader, and by passing

data packages known as application protocol data units (APDUs) using the reader (Col. 1, line 63

– Col. 2, line 13 & Col. 9, lines 1-6), which meets the limitation of at least one PSD comprising

means for functionally connecting to said PSD interface and mans for functionally

communicating through said interface, PSD communications means for transmitting and

receiving APDU messages through said PSD interface. When a user attempts to access ISP

services from the token device, the ISP issues a challenge to the token device to ensure that the

user should be granted access to the ISP services (Col. 2, lines 16-23 & Col. 10, lines 24-33),

which meets the limitation of PSD processing means for interpreting said APDU messages,

executing commands included in said APDU messages. Once the challenge is received at the

token device, the token device issues a response to the ISP challenge in the form shown in Figure

8B (Col. 10, lines 33-35), which meets the limitation of transmitting responses in APDU format

through said PSD interface using said communications means. The secure token device contains

a unique ID that is encoded into the token device (Col. 10, lines 54-55), which meets the

limitation of memory storage means for storing at least one unique identifier.

Referring to claim 3, DiGiorgio discloses that when a user attempts to access ISP services

from the token device, the ISP issues a challenge to the token device to ensure that the user

should be granted access to the ISP services (Col. 2, lines 16-23 & Col. 10, lines 24-33), which

meets the limitation of server communications means for transmitting and receiving messages

over said network using said packet based communications protocol, first server data processing

means for receiving requests from at least one applications level program, translating said

requests into APDU format and transmitting said APDU formatted requests to a second server

data processing means, second server data processing means for encapsulating said APDU

formatted requests received from said first server data processing means into outgoing message

packets and transmitting said outgoing message packets over said network to said local client

using said server communications means. Once the challenge is received at the token device, the

token device issues a response to the ISP challenge in the form shown in Figure 8B (Col. 10,

lines 33-35), which meets the limitation of third server data processing means for receiving

incoming messages from said local client using said server communications means and

separating encapsulated APDUs from said incoming message packets thus generating

desencapsulated APDUs and routing said desencapsulated APDUs to a fourth server data

processing means, and fourth server data processing means for receiving and translating said

desencapsulated APDUs sent by said third server data processing means into another message

format thus generating a translated message and transmitting said translated message to at least

one applications level program. DiGiorgio does not specify that the APDUs are encapsulated into

data packets, and deencapsulated from data packets. However, it would have been obvious to one

of ordinary skill in the art at the time the invention was made to encapsulate the packets

transmitted from the local computer to the remote computer in DiGiorgio using SSL in order to

provide a security in communications over networks that is platform independent, that can work

with many different types of applications that request a wide variety of different types of server

applications, and which can be performed with minimal time and effort as taught by Elgamal

(Col. 1, lines 11-19, 39-55).

Referring to claim 4, DiGiorgio discloses that the network can be the Internet (Col. 1,

lines 19-20), which meets the limitation of a public network.

Referring to claim 5, DiGiorgio discloses that the network can be a LAN (Col. 7, lines

28-29), which meets the limitation of a private network.

Referring to claim 6, DiGiorgio discloses that the communications protocol is the Internet

Protocol (Col. 1, lines 38-39), which meets the limitation of an open communications protocol.

Referring to claim 7, DiGiorgio discloses that the communications can be encrypted (Col.

11, lines 21-25), which meets the limitation of a secure communications protocol.

Referring to claim 9, DiGiorgio discloses a secure token device access system wherein a

secure token device and a local computer system communicate via a token reader, and by passing

data packages known as application protocol data units (APDUs) using the reader (Col. 1, line 63

– Col. 2, line 13 & Col. 9, lines 1-6), which meets the limitation of PSD communications means

for transmitting and receiving encrypted APDU messages through said PSD interface. When a

user attempts to access ISP services from the token device, the ISP issues a challenge to the

token device to ensure that the user should be granted access to the ISP services (Col. 2, lines 16-

23 & Col. 10, lines 24-33). The computer system utilizes Netscape Navigator, which includes

SSL capabilities and would therefore enable two way encrypted communications (Col. 7, lines

44-47), which meets the limitation of first PSD processing means for decrypting incoming

encrypted APDU messages using stored cryptographic information, thus generating incoming

decrypted APDU messages, second PSD processing means for interpreting said incoming

decrypted APDU messages, and executing commands included in said incoming decrypted

APDU messages, third PSD processing means for encrypting outgoing APDU response

messages using stored cryptographic information thus generating outgoing encrypted APDU

response messages, and transmitting said outgoing encrypted APDU response messages in said

APDU format through said PSD interface using said communications means, means for storing

at least one cryptographic key. The secure token device contains a unique ID that is encoded into

the token device (Col. 10, lines 54-55), which meets the limitation of memory storage means for

storing at least one unique identifier.

Referring to claims 10, 15, DiGiorgio discloses a secure token device access system

wherein a secure token device and a local computer system communicate via a token reader, and

by passing data packages known as application protocol data units (APDUs) using the reader

(Col. 1, line 63 – Col. 2, line 13 & Col. 9, lines 1-6), which meets the limitation of server

communications means for transmitting and receiving messages over said network using said

packet based communications protocol. Once the challenge is received at the token device, the

token device issues a response to the ISP challenge in the form shown in Figure 8B (Col. 10,

lines 33-35). The computer system utilizes Netscape Navigator, which includes SSL capabilities

and would therefore enable two way encrypted communications (Col. 7, lines 44-47), which

meets the limitation of cryptography data processing means, first server data processing means

fro receiving requests from at least one applications level program, translating said requests into

APDU format and transmitting said APDU formatted requests to said cryptography data

processing means, second server data processing means for encapsulating encrypted APDU

formatted requests received from said cryptography data processing means into outgoing

message packets transmitting said outgoing message packets over said network using said server

communications means, third server data processing means for receiving incoming message

packets using said server communications means and separating encapsulated APDUs from said

incoming message packets thus generating desencapsulated APDUs and routing said

desencapsulated APDUs to said cryptography data processing means, fourth server data

processing means for receiving and translating decrypted desencapsulated APDUs send by said

cryptography processing means into another message format thus generating a translated

message and transmitting said translated message to at least one applications level program,

wherein said cryptography data processing means comprises means for encrypting said APDU

formatted requests received from said first server data processing means and sending said

encrypted APDU formatted requests to said second server data processing means and for

decrypting said desencapsulated APDUs received from said third server data processing means

and sending said decrypted desencapsulated APDUs to said fourth server data processing means.

DiGiorgio does not specify that the APDUs are encapsulated into data packets, and

deencapsulated from data packets. However, it would have been obvious to one of ordinary skill

in the art at the time the invention was made to encapsulate the packets transmitted from the

local computer to the remote computer in DiGiorgio using SSL in order to provide a security in

communications over networks that is platform independent, that can work with many different

types of applications that request a wide variety of different types of server applications, and

which can be performed with minimal time and effort as taught by Elgamal (Col. 1, lines 11-19,

39-55).

Referring to claims 16, 17, 19, DiGiorgio discloses that the network can be a cellular

network (Col. 5, line 39), which meets the limitation of a digital cellular network and a wireless

network.

Referring to claims 20, 28, 37, DiGiorgio discloses a secure token device access system

wherein a secure token device and a local computer system communicate via a token reader, and

by passing data packages known as application protocol data units (APDUs) using the reader

(Col. 1, line 63 – Col. 2, line 13 & Col. 9, lines 1-6), which meets the limitation of generating a

request to access said PSD on said remote computer system, wherein said request is in a non-

native protocol for communicating with said PSD and said request is generated by an API level

program, converting on said remote computer system said request from said non-native protocol

into an APDU format request message using a first server data processing means. When a user

attempts to access ISP services from the token device, the ISP issues a challenge to the token

device to ensure that the user should be granted access to the ISP services (Col. 2, lines 16-23 &

Col. 10, lines 24-33), which meets the limitation of on said remote computer system said APDU

format request message into said packet based communications protocol producing an

encapsulated request message, using a second server data processing means, transmitting said

request message over said network using said packet based communications protocol. Once the

challenge is received at the token device, the token device issues a response to the ISP challenge

in the form shown in Figure 8B (Col. 10, lines 33-35), which meets the limitation of receiving by

said client said request message sent over said network, processing said request message using a

first data processing means to separate said APDU format request message from said request

message, routing on said client said APDU format request message through a hardware device

port assigned to a PSD interface independently of the origin and integrity of said encapsulated

request message, wherein said PSD interface is in processing communication with said PSD,

receiving by said PSD said APDU format request message through said PSD interface and

processing said APDU format response message into said packet based communications protocol

producing an response message, using a second data processing means, transmitting said

response message over said network using said packet based communications protocol, receiving

said response message sent over said network by said remote computer system, processing said

response message using a third server data processing means to separate said APDU response

message from said response message thus generating a APDU response message, converting by

said remote computer system said APDU response message into a response in a non-native

protocol using a fourth server data processing means and forwarding said response to at least one

API level program. DiGiorgio does not specify that the APDUs are encapsulated into data

packets, and deencapsulated from data packets. However, it would have been obvious to one of

ordinary skill in the art at the time the invention was made to encapsulate the packets transmitted

from the local computer to the remote computer in DiGiorgio using SSL in order to provide a

security in communications over networks that is platform independent, that can work with many

different types of applications that request a wide variety of different types of server

applications, and which can be performed with minimal time and effort as taught by Elgamal

(Col. 1, lines 11-19, 39-55).

Referring to claim 21, DiGiorgio discloses that the network can be the Internet (Col. 1,

lines 19-20), which meets the limitation of a public network.

Referring to claim 22, DiGiorgio discloses that the network can be a LAN (Col. 7, lines 28-29), which meets the limitation of a private network.

Referring to claim 23, DiGiorgio discloses that the communications protocol is the Internet Protocol (Col. 1, lines 38-39), which meets the limitation of an open communications protocol.

Referring to claim 24, DiGiorgio discloses that the communications can be encrypted (Col. 11, lines 21-25), which meets the limitation of a secure communications protocol.

Referring to claim 25, DiGiorgio discloses that system may automatically attempt to grant the user access to the ISP services once the token device is authenticated (Col. 10, lines 24-28), which meets the limitation of said communication pipe is initiated automatically upon connection of said PSD to said local client.

Referring to claims 26, 27, DiGiorgio discloses that the access to the ISP services may be granted upon a user double click on an icon associated with the ISP (Col. 10, lines 24-26), which meets the limitation of said communications pipe is initiated by a client requesting access to information contained on one or more networked clients or networked remote computer systems.

Referring to claims 29, 36, 37, DiGiorgio discloses a secure token device access system wherein a secure token device and a local computer system communicate via a token reader, and by passing data packages known as application protocol data units (APDUs) using the reader (Col. 1, line 63 – Col. 2, line 13 & Col. 9, lines 1-6), which meets the limitation of generating a request to access said PSD on said remote computer system, wherein said request is in a non-native protocol for communicating with said PSD and said request is generated by an API level program, converting on said remote computer system said request from said non-native protocol

into an APDU format request message using a first server data processing means, and sending

said APDU format request message to a cryptography data processing means. When a user

attempts to access ISP services from the token device, the ISP issues a challenge to the token

device to ensure that the user should be granted access to the ISP services (Col. 2, lines 16-23 &

Col. 10, lines 24-33). The computer system utilizes Netscape Navigator, which includes SSL

capabilities and would therefore enable two way encrypted communications (Col. 7, lines 44-

47), which meets the limitation of receiving and encrypting said APDU format request message

using cryptography data processing means thus generating an encrypted APDU request message

and sending said encrypted APDU request message to a second server data processing means,

wherein said cryptography data processing means uses a pre-established encryption method, on

said remote computer system said encrypted APDU request message into said packet based

communications protocol producing an and encrypted request message, using said second server

data processing means, transmitting said and encrypted request message over said network using

said packet based communications protocol. Once the challenge is received at the token device,

the token device issues a response to the ISP challenge in the form shown in Figure 8B (Col. 10,

lines 33-35), which meets the limitation of receiving said encapsulated and encrypted request

message sent over said network by said client, processing said and encrypted request message

using a first client data processing means to separate said encrypted APDU request message from

said and encrypted request message thus generating a encrypted APDU request message, routing

on said client said encrypted APDU request message through a hardware device port assigned to

a PSD interface independently of the origin and integrity of said and encrypted request message,

wherein said PSD interface is in processing communication with said PSD, receiving said

encrypted APDU request message through said PSD interface by said PSD and decrypting said

encrypted APDU request message using an internal PSD data cryptography means thus

generating a and decrypted APDU request message, wherein said cryptography means is pre-

established and sending said and decrypted APDU request messages to a first internal PSD data

processing means, receiving said and decrypted APDU request message from said internal PSD

data cryptography means and processing said desencapsulated and decrypted APDU request

message using said first internal PSD data processing means, generating a response message in

APDU format by said PSD using a second internal PSD data processing means, encrypting said

APDU format response message using said internal PSD data cryptography means thus

generating an encrypted APDU format response message response message through said PSD

interface, and transmitting said encrypted APDU format receiving by said client said encrypted

APDU format response message through said PSD Interface and said encrypted APDU format

response message into said packet based communications protocol producing an and encrypted

response message, using a second client data processing means, transmitting said message over

said network using and encrypted response said packet based communications protocol,

receiving by said remote computer system said and encrypted response message sent over said

network, processing said and encrypted response message using a third server data processing

means to separate said encrypted APDU response message from said and encrypted response

message thus generating a encrypted APDU response message, decrypting said encrypted APDU

response server data processing means message received from said third using said

cryptography data processing means thus generating a and decrypted APDU response message

and sending said and decrypted APDU response message to said fourth server data processing

means, and converting by said remote computer system said and decrypted APDU response

message into a response in a non-native protocol using a fourth server data processing means,

and forwarding said response to at least one API Level Program. DiGiorgio does not specify that

the APDUs are encapsulated into data packets, and deencapsulated from data packets. However,

it would have been obvious to one of ordinary skill in the art at the time the invention was made

to encapsulate the packets transmitted from the local computer to the remote computer in

DiGiorgio using SSL in order to provide a security in communications over networks that is

platform independent, that can work with many different types of applications that request a

wide variety of different types of server applications, and which can be performed with minimal

time and effort as taught by Elgamal (Col. 1, lines 11-19, 39-55).

Referring to claim 30, DiGiorgio discloses that the network can be the Internet (Col. 1,

lines 19-20), which meets the limitation of a public network.

Referring to claim 31, DiGiorgio discloses that the network can be a LAN (Col. 7, lines

28-29), which meets the limitation of a private network.

Referring to claim 32, DiGiorgio discloses that the communications protocol is the

Internet Protocol (Col. 1, lines 38-39), which meets the limitation of an open communications

protocol.

Referring to claim 33, DiGiorgio discloses that the communications can be encrypted

(Col. 11, lines 21-25), which meets the limitation of a secure communications protocol.

Referring to claims 34, 35, DiGiorgio discloses that the access to the ISP services may be

granted upon a user double click on an icon associated with the ISP (Col. 10, lines 24-26), which

meets the limitation of said communications pipe is initiated by a client requesting access to

information contained on one or more networked clients or networked remote computer systems.

Referring to claims 38, 39, 41, DiGiorgio discloses that the network can be a cellular

network (Col. 5, line 39), which meets the limitation of a digital cellular network and a wireless

network.

5.   Claims 18, 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over over

DiGiorgio, U.S. Patent No. 6,385,729, in view of of Elgamal, U.S. Patent No. 5,657,390 as

applied to claims 1, 20 above, and further in view of Brown, U.S. Patent No. 5,455,863.

Referring to claims 18, 40, DiGiorgio does not disclose that the network can be optical. Brown

discloses a network authentication system wherein the network is wireline, optical fiber link,

satellite, or any other type of communication channel (Col. 8, lines 56-58). It would have been

obvious to one of ordinary skill in the art at the time the invention was made for the network of

Chan to be optical because Brown discloses that those skilled in the art would understand that

different networks can be used without departing from the spirit and scope of the invention (Col.

8, lines 48-55).

Double Patenting

6.   The nonstatutory double patenting rejection is based on a judicially created doctrine

grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or

improper timewise extension of the "right to exclude" granted by a patent and to prevent possible

harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed.

Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686

F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA

1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

7.   A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to

overcome an actual or provisional rejection based on a nonstatutory double patenting ground

provided the conflicting application or patent is shown to be commonly owned with this

application. See 37 CFR 1.130(b).

8.   Effective January 1, 1994, a registered attorney or agent of record may sign a terminal

disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37

CFR 3.73(b).

9.   Claims 1-7, 9, 10, 15-42 are provisionally rejected under the judicially created doctrine of

obviousness-type double patenting as being unpatentable over claims 1-4, 7-10, 13-15 of

copending Application No. 09/844,439, '439 application. Although the conflicting claims are

not identical, they are not patentably distinct from each other because both applications claim

methods and systems for transmitting message packets, by a remote computer system, with

encapsulated APDUs over a communication path to a local client that desencapsulates the

message packets before routing the APDUs to the PSD. The PSD then routs APDUs to the local

client for encapsulation and transmission to the remote computer system. The methods and

systems containing encrypted and unencrypted embodiments. Therefore claims 1-42 of the

current application are anticipated in claims 1-4, 7-10, 13-15 of the '439 application.
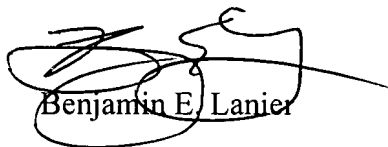
        This is a <u>provisional</u> obviousness-type double patenting rejection because the conflicting

claims have not in fact been patented.

Conclusion

10.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805.

The examiner can normally be reached on M-Th 6:00am-4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Benjamin E. Lanier